IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

-v- 16-CR-6084DGL

SCOTT T. WILBERT,

Defendant.

GOVERNMENT'S POST HEARING MEMORANDUM

The defendant, SCOTT T. WILBERT, through his attorney, Robert A. Napier, Esq., has filed a post hearing memorandum in the above referenced matter. The UNITED STATES OF AMERICA, by and through its attorneys, James P. Kennedy, Jr., United States Attorney for the Western District of New York, and Melissa M. Marangola, Assistant United States Attorney, of counsel, hereby files the government's post hearing memorandum.

INDICTMENT

The defendant is charged in a one-count Indictment charging a violation of Title 18, United States Code, Section 2252A(a)(2)(A), knowingly receiving child pornography. Based on the defendant's prior conviction for sexual conduct involving a minor, pursuant to Title 18, United States Code, Section 2252A(b)(1), the defendant faces a mandatory minimum sentence of fifteen years (15) imprisonment and a maximum sentence of forty (40) years imprisonment.

STATEMENT OF FACTS

Omegle.com is an instant messaging/chat website created by Leif K-Brooks in 2009. (Hearing Transcript, January 17, 2018, hereinafter "HT", p. 21). The site is unique because other websites are designed for users to chat with other individuals they know. Id. Omegle.com was designed for users to connect with other random users that are unknown to each other. Id. The user has no control over who they are selected to chat with on the site. (HT, pp. 21-22). The site's software chooses the users selected to chat with each other at random and some users could be law enforcement agents posing as regular users. (HT, p. 22).

Leif K-Brooks published Omegle.com's privacy policy online in 2014 and it continues to remain in effect. (HT, pp. 25-27.) The site also contains a link to the privacy policy directly above the button a user would use to begin a chat session. (HT, p. 22.) The policy advises users that at the beginning of every chat (video or text) a record is made that includes the users' IP addresses and a timestamp of the chat. (Government Exhibit 3; HT, pp. 29, 31-32). This information is typically stored for approximately 120 days. (HT, p. 31, 34; See government exhibit 4).

Additionally, the site issues a warning in large text on the site that advises users that the video chats are moderated. (HT, p. 23.) The video chats operate on a peer-to-peer system, which means the video transmissions never travel through Omegle servers. (HT, pp. 27-28). The video moderation system captures screenshots of the video chats, which are reviewed by the moderation system and then human moderators. (HT, p. 29). More specifically, the moderation system has automated software that captures screenshots from the video chats that are uploaded to Omegle's servers, screens them for unwanted content, and sends them to a queue for human moderation review if they fail the automated test. (HT, p. 34).

The automated software program flagged two images from the defendant's IP address (50.49.31.78) on October 25, 2015 at 2:30 and 2:36. (HT, p.38). The two images were captured from the user's computer and uploaded to Omgele's servers for moderation purposes. (HT, pp., 39-40). These images failed the automated screening test and were placed into a queue for human review of a private, third party moderation service, Gracall International. (HT, pp. 40-42). Omegle's metadata records show information related to the two jpge images including that they were captured from the defendant's IP address and how they were classified by the moderators. (HT, p. 42; Governments Exhibits 5 & 6).

The jpeg image uploaded by the defendant's IP address and saved to the Omgele server at 2:36 is saved as jpeg "c6do". (HT, pp. 45-46). Metadata shows that specific image was flagged by the automated software as suspicious then reviewed by a human moderator with employee ID "Gracall115", who flagged the image by pressing a button saying she believed the image contained child pornography. (HT, p. 46). Jpeg image "a9e7" was uploaded by the defendant's IP address at 2:30 and flagged by the automated moderation system. (HT, pp. 47, 49). The metadata can confirm whether or not a human moderator actually viewed the image because the image was not flagged by a human as containing child pornography. (HT, pp. 49-50).

Once jpeg image "c6d0" was flagged by a human moderator as containing child pornography, a software program designed by Omegle automatically sent a cybertip to NCMEC. (HT, pp. 50-52, 54-55). In this case, the cybertip sent by Omegle created NCMEC Cybertip Report 6928493, which contained both jpeg images uploaded by the defendant's IP address on October 25, 2015 at 2:30 and 2:36. (Government Exhibit 7; HT, p. 55). Cybertip Report 6928493 accurately states that jpeg image "c6d0" was opened by a human moderator. (Government Exhibit 7, p. 3; HT, pp. 57-58). The cybertip report does not indicate that jpeg image "a9e7" was opened by a human moderator. (HT, pp. 57-58; Government Exhibit 7, p. 2). Omegle.com has no further involvement with the images after a cybertip is submitted to NCMEC. (HT, p. 58).

Leif K-Brooks explained that he does not believe that he has to actively look on Omegle.com for images of child pornography. (HT, p. 50). He understands that if he sees child pornography on Omegle.com, he has to report the images to NCMEC, which is what he did in this case. (HT, p. 50). NCMEC received Omegle's cybertip related to this case on October 25, 2015 at 2:38:58. (HT, p. 111, Government Exhibit 7). NCMEC Vice President John Sheehan reviewed Cybertip Report 6928493 and explained Section A of the report is information submitted directly by Omegle (HT, pp. 112-113). He confirmed that Omegle submitted two jpeg images to the cybertipline that were uploaded by IP address 50.49.31.78 and the timestamps of the uploads. (HT, p. 113, 115-116).

Sheehan explained that based on the information provided by Omegle, NCMEC could not determine that jpeg image "a9e7" had been previously opened by a human moderator. (HT, p. 114). Omegle did indicate however, that jpeg image "c6d0" was opened previously by a human moderator. (HT, p. 115). Once the information was submitted to NCMEC, NCMEC then used a public website to determine the geographical location of the IP address. (HT, p. 116). NCMEC commonly uses MaxMind to find the geographical location because it is free, reliable and works quickly. (HT, pp. 116-117, 159). NCMEC used this software to determine the IP address related to this matter was located in Rochester, New York and is affiliated with Frontier Communications. (HT, p. 117). NCMEC does this public search so it can pass the information on to the appropriate law enforcement agency. (HT, pp. 118-119, 159).

Sheehan reviewed the Cybertip Report in this case and reviewed jpeg image "c6d0" as it was the only viewable image that he had access to. (HT, p. 120). Jpeg image "a9e7" had never been previously viewed by any NCMEC employee because of software that prevented the image from being opened. (HT, p. 120). In 2014, NCMEC implemented software that prohibits employees from viewing images that had not been previously viewed by the submitting company, in this case Omegle. (HT, pp 120-121). Since Omegle submitted information to NCMEC that jpeg image "a9e7" had not been previously viewed, NCMEC locked the image in its system and made that image unviewable. (Government Exhibit 9; HT, pp. 120-122, 151-152). For an employee to be able to view that image, the employee would need an override authorization code; Sheehan confirmed that did not occur here with respect to image "a9e7". (HT, p. 122, 154-155).

Image “c6d0” was available to be viewed by a NCMEC employee because Omegle indicated in its submission that the image had been previously opened by a human moderator. (HT, p. 128). Sheehan personally observed image “c6d0” in the Cybertip Report and confirmed this image was Government Exhibit 1 at the hearing. (HT, p. 128). The “image” is actually a screenshot contained of 4 still images taken from the video chat. (HT, p. 129). Sheehan described image “c6d0” as being a girl between 4-7 years old receiving oral sex from a dog. (Government Exhibit 1; HT, p. 130). Government Exhibit 2 was confirmed to be image “a9e7”, which was never seen by Sheehan prior to that date. (HT, p. 130).

Sheehan could determine from the Cybertip Report that an employee had viewed image “c6d0” and marked it as “child pornography unconfirmed” which tells him the employee could not make a determination of the child’s age. (HT, p. 131). NCMEC does not have the authority to make determinations as to whether a specific image is considered child pornography; law enforcement has the responsibility to make that determination. (HT, p. 133). These images and the report were then made available to the New York State Police via a virtual private network that can only be accessed by NCMEC and the corresponding law enforcement agencies. (HT, p. 133). There are no restrictions placed on any images as they are passed on to law enforcement and NCMEC has no control over what law enforcement views. (HT, pp-135-136).

New York State Police (NYSP) investigators then accesses the web portal and viewed Cybertip Report 6928493 along with both jpeg images submitted with the report. (HT, p. 166).

Both images were viewed to determine whether one or both met the statutory requirements for criminal offenses related to child pornography. (HT, pp. 166-167). NYSP investigators make their own determination as to this issue and do not rely on other non-law enforcement opinions for this issue. (HT, pp. 166-167, 191-191). NYSP then issued subpoenas to Frontier Communications to determine who the relevant IP address belonged to. (HT, p. 167).

On approximately December 22, 2015, the case was assigned to NYSP Investigator Dave Cerretto for further investigation. (HT, pp. 167-168). Investigator Cerretto viewed the Cybertip Report along with both jpeg images. (HT, pp. 168-169). He viewed image "c6d0" and confirmed it contained child pornography, specifically a young girl receiving oral sex from a dog. (HT, pp. 169-170; Government Exhibit 1). He viewed image "a9e7" and could not determine if it contained child pornography or not. (HT, p. 170; Government Exhibit 2).

Based on his personal review of the images, he sought a search warrant for the defendant's residence at 634 Garson Avenue, upstairs. (Government Exhibit 12; HT, pp. 170-171). In the application, Investigator Cerretto lists his facts in support of probable cause to be his review of Cybertipline Report 6928493 and describes the image he identified as Government Exhibit 1, image "c6d0", which is a young girl between 4 and 7 years old engaged in oral sex with a K-9. (Government Exhibit 12; HT, pp. 172-172, 187). The warrant application describes the image to be uploaded by the defendant's IP address at 2:30. (HT, p 173). It is uncontested that image "c6d0" was actually uploaded by the defendant's IP address at 2:36. (HT, p. 173; Government Exhibits, 5, 6 & 7). Investigator Cerretto explained that he considered the incident related to both images to be one continuous act, beginning at 2:30, the time the first image ("a9e7") was uploaded by Omegle from the defendant's video chat. (HT, pp. 173-174; 178-179, 185, 189). He made clear that he applied for the search warrant based on image "c6d0", which he determined to contain child pornography. (HT, p. 174). Monroe County Court Judge Victoria Argento then authorized a search warrant for the defendant's residence based on Investigator Cerretto's application. (Government Exhibit 12; HT, p. 174).

DISCUSSION

Omgele Conducted a Private Search

The Fourth Amendment regulates state actors. Private parties are only bound by its requirements insofar as they operate as state actors. The Fourth Amendment is "wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as a defacto agent of the government." United States v. DiTomasso, 81 F.Supp 3d 304, 308 (SDNY 2015), citing United States v. Jacobsen, 466 U.S. 109, 104 S.Ct. 1652 (1984); Coolidge v. New Hampshire, 403 U.S. 443, 487-89, 91 S. Ct. 2022 (1971). A private citizen may act as an agent for the government if the party *must* perform a search, or fact liability for not doing so. Skinner v. Railway Labor Executives Ass'n, 489 U.S. 602, 614 (1989).

It is well established that privately owned ISP's, including Omegle.com are not government actors. United States v. DiTomasso, 81 F.Supp 3d 304, 310 (SDNY 2015); See United States v. Richardson, 607 F.3d 357, 364 (4th Cir. 2010); United States v. Stevenson, 727 F.3d 826, 829-30 (8th Cir. 2013); United States v. Keith, 980 F.Supp.2d 33, 40 (D.Mass. 2013); United States v. Ackerman, 2014 WL 2968164,*6-7 (D.Kan., July 1, 2014). See also United States v. Drivdahl, 2014 WL 896734 (D.Mont., Mar. 6, 2014) (holding that a different internet service provider, Google, was not an agent of the government in reporting apparent images of child pornography to NCMEC). The defendant concedes this fact by failing to raise a contrary argument in his filing. Omegle.com is a privately owned business, founded by Leif K-Brooks in 2009. (HT, p. 21). Omegle.com began monitoring chats in 2012 in an effort to remove the inappropriate content flowing through its site after receiving bad publicity when individuals used the site to meet minors. DiTomasso, 81 F.Supp 3d at 310. K-Brooks felt no legal obligation to monitor his site for child pornography or other inappropriate conduct; he did so on his own accord. Id. K-Brooks was aware that if he did find any child pornography on his site, only then did he have a duty to *report* this to NCMEC. Id. (HT, pp. 50-51). K-Brooks "appreciates the difference between an obligation to monitor and an obligation to report" and correctly understands Section 2258A as imposing no duty to monitor". Id.

In this case, the monitoring software designed by K-Brooks flagged two images sent by the defendant's IP address as being suspicious of containing inappropriate content. (HT, p. 38) The images flagged were jpeg image "a9e7" and jpeg image "c6d0". Id. Omegle's metadata confirmed that jpeg image "c6d0" was viewed by a third party human moderator. (HT, p. 44; Government

Exhibits 5 & 6). The human moderator pressed a button that indicated the human moderator believed that image "c6d0" contained child pornography. (HT, p. 46.) The metadata also showed that image "c6d0" was uploaded by the defendant's IP address at 2:36:12. Id. Further, the metadata showed that image "a9e7" was uploaded by the defendant's IP address at 2:30:21, but it did not confirm that the image was actually viewed by a third party human moderator. (HT, p. 49; Government Exhibits 5 & 6). Based on the human moderator's determination that image "c6d0" contained child pornography and her action of "flagging" the image by pressing a button, the image was sent to a queue which automatically submitted Cybertip Report 6928493 containing both images. (HT, pp. 51,53, 55; Government Exhibit 7).

K-Brooks created the software that monitored the site for inappropriate content and hired the third party moderation service on his own accord. He specifically designed software to capture the images sent from users' computers to be uploaded onto Omegle's servers for the purpose of moderation. (HT, pp. 39-40) The third party moderation service used by Omegle is a privately owned company called Gracall International. (HT, pp. 40-41.) Gracall International provides moderation services for other companies including competitors of Omegle. (HT, p. 41).

Consistent with the ruling in DiTomasso, K-Brooks' testimony here was clear that the moderation of Omegle.com was done on his own accord. 81 F.Supp 3d at 311. Jpeg image "c6d0" was flagged by Omegle's automated software and then actually viewed by a private third party human monitor prior to the image being sent to NCMEC. This was done without any involvement of law enforcement, nor was there any legal requirement for Omegle to search his site for child pornography. Therefore, the search of image "c6d0" by Omegle's software and third party human moderator raises no Fourth Amendment concern. Id.

NCMEC did not Expand Omegle's Private Search

The government continues to maintain that NCMEC is not a government entity. John Sheehan, Vice President of NCMEC's Exploited Child Division detailed how NCMEC conducts its business as a private entity. (HT, pp. 98-99, 109, 124-127). NCMEC is a non-for profit private entity that received funding through a variety of sources including federal grants, corporate monetary donations and in-kind donations. (HT, pp. 101-102). The Cybertipline was actually created entirely through an in-kind private donation from Sun Micro Systems. (HT, p. 102). The current cybertipline evolved from a telephone line that served the same purpose but became outdated as technology advanced. (HT, p. 103). That tip line had absolutely no government or law enforcement involvement. (HT, pp. 103-104). The Articles of Incorporation (Government Exhibit 8) further confirm the organization is run as a private entity. (HT, p. 109).

There is no question that NCMEC works closely with law enforcement and have federal reporting requirements and other regulations as do many other private organizations This close relationship and federal funding does not automatically make the private entities "government agents". However, to error on the side of caution after the 8th Circuit found NCMEC to be government entity, NCMEC made significant changes to its practice to distinguish itself from law enforcement. (HT, p. 125). NCMEC removed all law enforcement officers from its board of directors and has prevented law enforcement from having access to NCMEC employees on a regular basis. (HT, p. 126).

Most important to this case, NCMEC implemented software to ensure they never exceed the scope of the searches done by submitting ISPs. (HT, pp. 120-122). Sheehan carefully explained NCMEC's process of receiving and processing cybertips in general. Sheehan then went through Cyber Tip Report 6928493 in detail and demonstrated how the NCMEC employee who processed this tip only personally viewed jpeg image "c6d0", an image previously viewed by a human moderator and had no access to image "a9e7", a previously unopened image. (HTpp. 120-121). Sheehan also detailed how NCMEC uses public websites including MaxMind to determine the geographical location of the IP address in question. (HT, pp. 116-117). Utilizing publicly available information does not expand Omegle's search. United States v. Jones, 565 U.S 400, 132 S. Ct. 945 (2012); (HT, p. 197).

Since NCMEC never did anything but replicate the conduct done by Omegle.com and use a public website to determine geographical information for the IP address, it is irrelevant whether or not they are a government actor or a private entity. Thus, the Court need not decide that issue in this case.

The New York State Police's Actions did not Exceed Omegle's Private Search.

It is undisputed that the NYSP opened both images submitted by NCMEC in Cybertipline Report 6928493 despite the fact that image "a9e7" had not previously been opened by Omegle's human moderator or NCMEC. It is their customary practice to open all images submitted by NCMEC to confirm the images meet the statutory definition of child pornography. (HT, pp. 190-191). Despite opening image "a9e7", the government maintains NYSP did not exceed Omegle's private search.

The private search doctrine permits a government agent to verify the illegality of evidence discovered during a private search provided the agent stays within the scope of the private search. United States v. Jacobsen, 466 U.S. at 119-20); United States v. Lichtenberger, 786 F.3d 478, 481-83 (6th Cir. 2015). A government agent's invasion of a defendant's privacy must "be tested by the degree to which [the agent] exceeded the scope of the private search." Jacobsen, 466 U.S. at 115 (citing Walter, 447 U.S. 649). "Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-non-private information." Id., at 117. Under the private search doctrine, the critical measure of whether a government search exceeds the scope of the private search that preceded it are how much information the government stands to gain when it re-examines the evidence and relatedly, how certain it is regarding what it will find." United States v. Miller, 2017 WL2705963 (E.D.K.Y, 2017), citing Lichtenberger, 786 F.3d at 485-86; Jacobsen, 466 U.S. at 119.

The Court here must determine whether the Fourth Amendment is implicated by the NYSP's opening and viewing of the images provided by NCMEC in Cybertipline Report 6928493. Employees at Omegle and NCMEC previously reviewed one of the two images that were flagged by the automated software. The opened image was captured by the automated software on October 25, 2015 at 2:30 a.m. The second image viewed by the NYSP was flagged by the automated software at 2:36, identified as suspicious and determined to occur during the same chat session as the previous image. This still image was not personally viewed by an employee at Omegle or NCMEC, but was forwarded on the NYSP based on the connection to the other image and it being flagged by the automated software program as suspicious.

The defendant relies on the Ackerman decision to support his argument that the search by NYSP in this case was unconstitutional. There, the defendant sent an email containing child pornography that was intercepted by AOL before the email reached the intended recipient. Ackerman, 831 F.3d at 1294. The email had four attachments, one of which was flagged by the automated software program as being suspicious. Id. At no time did an actual employee review the contents of the email or any of the attachments. The email and all four attachments were reported to NCMEC. Id. A NCMEC employee opened the email and all four attachments, confirming that the images all contained child pornography. Id. The Ackerman court then concluded that NCMEC was a government agent and exceeded AOL's private search because NCMEC opened and viewed information beyond the one image that was the target of AOL's automated software. Id. at 1306. The Ackerman court's concern was solely with the fact that NCMEC opened an email *and* three other attachments that could have exposed "private, non-contraband information that AOL had not previously examined" including correspondence or personal details of the recipient of the email. Id. at 1306-07.

The facts of this case are distinguishable from Ackerman as there is no evidence that Omegle sent anything to NCMEC (or ultimately the NYSP) other than the two still images (as opposed to an unopened email with three additional unlagged attachments) that were captured by the automated software and flagged as suspicious. (HT, pp. 190-191). Thus, the reasoning of the Ackerman court finding the search exceeded the scope of the private search is not applicable in this case.

The issue is whether the NYSP's opening of the two images risked exposing any private information beyond what Omegle had reported to NCMEC. The answer is no. Omegle did not, as was the case in Ackerman, simply send the unopened video chat to NCMEC. Omegle actually captured two still images (4 still images each) from the video feed and uploaded these images to their servers. Image "c6d0" was actually viewed by a human moderator hired by Omegle before it was forwarded to NCMEC. A NCMEC employee viewed the same image and then forwarded it on to the NYSP who also viewed the image. Obviously, the private search was not expanded by NYSP with respect to this image. Image "a9e7" was flagged by Omegle's automated software as suspicious. A human moderator did not open this image but forwarded it along with the first image because it was flagged by the software and both images occurred during the same video chat. A

NCMEC employee did not view this image, but forwarded it on to the NYSP as part of Cybertipline Report 6928493.

NYSP Investigator Cerretto (and other NYSP investigators) opened both images to confirm they contained child pornography and he then continued his investigation by issuing subpoenas for the IP address associated with the images and ultimately a search warrant for the defendant's home. (HT, pp. 191-192). The images opened by the NYSP were simply the still captures of the video streamed by the defendant during the Omegle chat on October 25, 2015. These still images were flagged by Omegle's software, seized by Omegle and uploaded to Omegle's server. Unlike the email and attachments at issue in Ackerman, there was no additional correspondence or information contained in the two images.

The NYSP received the images in a Cybertipline Report from NCMEC, which is a notification that NYSP regularly receives specific to child pornography cases. When NYSP opened the images, it was for the sole purpose to confirm the images contained child pornography that would meet the legal criteria required for criminal charges. As in Jacobsen, there was a virtual certainty that nothing else of significance except child pornography would be found in the attachments and a manual search of the unopened file would reveal nothing more than Omegle's private search (through virtual technology) already revealed. (Jacobsen 466 U.S. at 120). Therefore, NYSP's activity falls within the private search doctrine and no Fourth Amendment violation occurred.

Assuming arguendo, the Court finds that NYSP did expand the private search as to image "a9e7", it is meaningless for this specific case. Perhaps in other cases with different facts, the actions of NYSP may be of concern. Here however, the only image of any importance is jpeg "c6d0". (Government Exhibit 1). It is undisputed that image "c6d0" was opened by an Omegle third party human moderator, and NYSP did not expand any search done with respect to that image. That particular image established the probable cause basis for the warrant. Therefore, it makes no difference what NYSP did with respect to image "a9e7" as it was not confirmed to contain child pornography and it was not used for establishing probable cause for the warrant.

Franks Analysis

The hearing testimony made clear there were no misrepresentations or falsehoods contained in the search warrant. (Government Exhibit 12). Investigator Cerretto testified that he personally reviewed image "c6d0" (Government Exhibit 1), which he determined to contain child pornography. He described the image in the application as being a young girl between 4 and 7 years old engaging in oral sex with a K-9. (HT, pp. 169-171). A review of the image, introduced at the hearing as Government Exhibit 1, shows his description was accurate. He explained that the application states the image was uploaded at 2:30 because he considered the defendant's actions related to the two images to be one ongoing incident, which began at 2:30 when the first image ("a9e7") was uploaded. (HT, pp. 188-189).

The defendant's claim that there was a fraudulent misstatement in the warrant application was completely undermined by the testimony at the hearing. Before submitting the affidavit for judicial consideration, Investigator Cerretto personally viewed the image in question and determined the girl was between 4 and 7 years old. (HT, pp. 169-171). He did not need to rely on the CyberTipline Report description because he had personal knowledge of what the photo contained.

In order to consider a Franks argument, a defendant challenging an affidavit must make "a substantial preliminary showing that (1) the affidavit contained false statements made knowingly or intentionally, or with reckless disregard for the truth; and (2) the challenged statements or omissions were necessary to the Magistrate's probable cause finding. United States v. Levasseur, 816 F.2d 37, 43 (2d Cir. 1987) (citing United States v. Franks, 438 U.S. at 154, 171-172 (1978)). A hearing is required only if the defendant provides the court with a sufficient basis upon which to doubt the truth of the affidavit at issue. As the Supreme Court has explained:

> To mandate an evidentiary hearing, the challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine. There must be allegations of deliberate falsehood or of reckless disregard for the truth, and those allegations must be accompanied by an offer of proof. They should point out specifically the portion of the warrant affidavit that is claimed to be false; and they should be accompanied by a statement of supporting reasons. Affidavits or sworn or otherwise reliable statements of witnesses should be furnished, or their absence satisfactorily explained.

Franks, 438 U.S. at 171.

With respect to the first prong, "allegations of negligence or innocent mistake are insufficient." Id. Instead, the focus is not on "whether a mistake was made, but rather on the intention behind the mistake." United States v. Markey, 131 F. Supp. 2d 316, 324 (D. Conn. 2001), aff'd, 69 F. App'x 492 (2d Cir. 2003). Thus, Franks teaches that not all statements in an affidavit have to be true; instead "the statements [must] be 'believed or appropriately accepted by the affiant as true.'" See United States v. Campino, 890 F.2d 588, 592 (2d Cir. 1989) (quoting Franks, 438 U.S. at 165).

With respect to omissions, "the mere intent to exclude information is insufficient. . . [because] 'every decision not to include certain information in the affidavit is 'intentional' insofar as it is made knowingly.'" United States v. Awadallah, 349 F.3d 42, 66 (2d Cir. 2003) (quoting United States v. Colkley, 899 F.2d 297, 300-301 (4th Cir. 1990)). Accordingly, "to have misled knowingly or recklessly, the government must have done more than make an intentional decision not to include the information; instead the misleading statement or omission must have been 'designed to mislead' or 'made in reckless disregard of whether [it] would mislead."' United States v. Rajaratnam, 2010 WL 4867402 at *8 (quoting United States v. Awadallah, 349 F.2d at 68).

To determine whether a misstatement in an affidavit is material, the court must "set aside the falsehoods in the application… and determine whether the untainted portions suffice to support a probable cause. . . finding." United States v. Rajaratnam, 719 F.3d 139, 146 (2d Cir. 2013). Although omissions are governed by the same rules as misstatements, the literal Franks approach is not appropriate because by their nature, omissions cannot be deleted; therefore the better approach in dealing with omissions is to insert the omitted truths and determine if the inclusion of such omissions would still support a finding of probable cause. Id., citing United States v. Ferguson, 758 F.2d 843, 848 (2d Cir.1985).

If the Court inserts the "omitted truths" in this case, the application would include the fact that Omegle's human moderator opened image "c6d0" and that NCMEC's employee opened the same image. (HT, pp. 46, 130). The application would then state that Investigator Cerretto opened the same image and it contained child pornography. (HT, pp. 169-170). Clearly, these facts would support a finding of probable cause. The only image that could possibly be suppressed in this case, is image "a9e7", which was not even mentioned in the warrant and is irrelevant to the judge's probable cause determination in issuing the warrant.

Accordingly, the defendant's argument fails.

Good Faith Doctrine

Should the court find NYSP's activity exceeded Omegle's private search with respect to jpeg image "c6d0", the government asserts that Investigator Cerretto acted in good faith in applying for the warrant in a subsequent filing. United States v. Leon, 468 U. S. 897 (1984). He received a NCMEC Cybertip Report with two images. He opened them for the sole purpose of confirming they contained child pornography. He reviewed image "c6d0 and observed a young girl engaging in oral sex with a dog. He then applied for a search warrant, using that image as a basis for establishing probable cause, in addition to information that the subscriber of the IP address, Scott T. Wilbert was a registered sex offender and was also investigated for previous allegations involving child pornography. He did everything correctly as it pertains to the only relevant image in this case, image "c6d0". The other image in question was not included in the warrant and has no relevance to this analysis.

Quite simply there was no law enforcement misconduct here that would warrant suppression of evidence in this case.

CONCLUSION

Based on the foregoing, it is submitted that the defendant's motion to suppress the evidence in this case be denied.

DATED: Rochester, New York, April 23, 2018.

Respectfully submitted,

JAMES P. KENNEDY, JR.
United States Attorney

By: s/Melissa M. Marangola
MELISSA M. MARANGOLA
Assistant U.S. Attorney
U.S. Attorney's Office
Western District of New York
100 State Street, Suite 500
Rochester, NY 14614
585/399-3925
Melissa.Marangola@usdoj.gov